Examiner Search Note:
09/884,636

reference not cited on PTO-1449

ATMEL
Secure Microcontrollers for Smart Cards

Features

- High-performance, Low-power 8-bit AVR® RISC Architecture
  - 120 Powerful Instructions
  - Most Single Clock Cycle Execution
- Up to 64K Bytes Flash Program Memory
  - Endurance: 10K Write/Erase Cycles
- Up to 64K Bytes EEPROM User Memory
  - Endurance: 250K Write/Erase Cycles
- Up to 2.5K Bytes RAM
- Cryptoprocessor
  - Pre-programmed Functions for Cryptography and Authentication
- Supervisor Mode (Memory Management)
- One or Two ISO 7816 I/O Ports
- Random Number Generator
- One or Two 16-bit Timers
- 2-level, 6-vector Interrupt Controller
- Security Features
  - Power-down Protection
  - Low-frequency and High-frequency Protection
  - Logical Scrambling on Program Code
- Low-power Idle and Power-down Modes
- Bond Pad Locations Conform to ISO 7816
- V_{CC}: 3.0V ± 10%, 5.0V ± 10%

Description

The AT90SC series is a low-power, high-performance, 8-bit microcontroller with Flash program memory and EEPROM data memory, based on the AVR RISC architecture. By executing powerful instructions in a single clock cycle, the AT90SC achieves throughputs close to 1 MIPS per MHz. Its Harvard architecture includes 32 general-purpose working registers directly connected to the ALU, allowing two independent registers to be accessed in one single instruction executed in one clock cycle.

Some products in the AT90SC family feature a cryptoprocessor: a 16-bit crypto engine dedicated to performing fast encryption or authentication functions (see table below). Additional security features include power and frequency protection logic, logical scrambling on program data and addresses, and memory accesses controlled by a supervisor mode.

The AT90SC family provides up to 128K bytes of Atmel's high-density, nonvolatile memory technology. The on-chip downloadable Flash allows the program memory to be reprogrammed in-system. This technology combined with the versatile 8-bit CPU on a monolithic chip provides a highly flexible and cost-effective solution to many smart card applications.

Table 1. The AT90SC Family

Device	Program Memory Flash Bytes	User Memory EEPROM Bytes	RAM Bytes	Crypto-processor	I/O Ports
AT90SC1616C	16K	16K	1K	Yes	2
AT90SC3232	32K	32K	1.5K	No	1
AT90SC3232C	32K	32K	1K	Yes	1
AT90SC6464C	64K	64K	2.5K	Yes	2

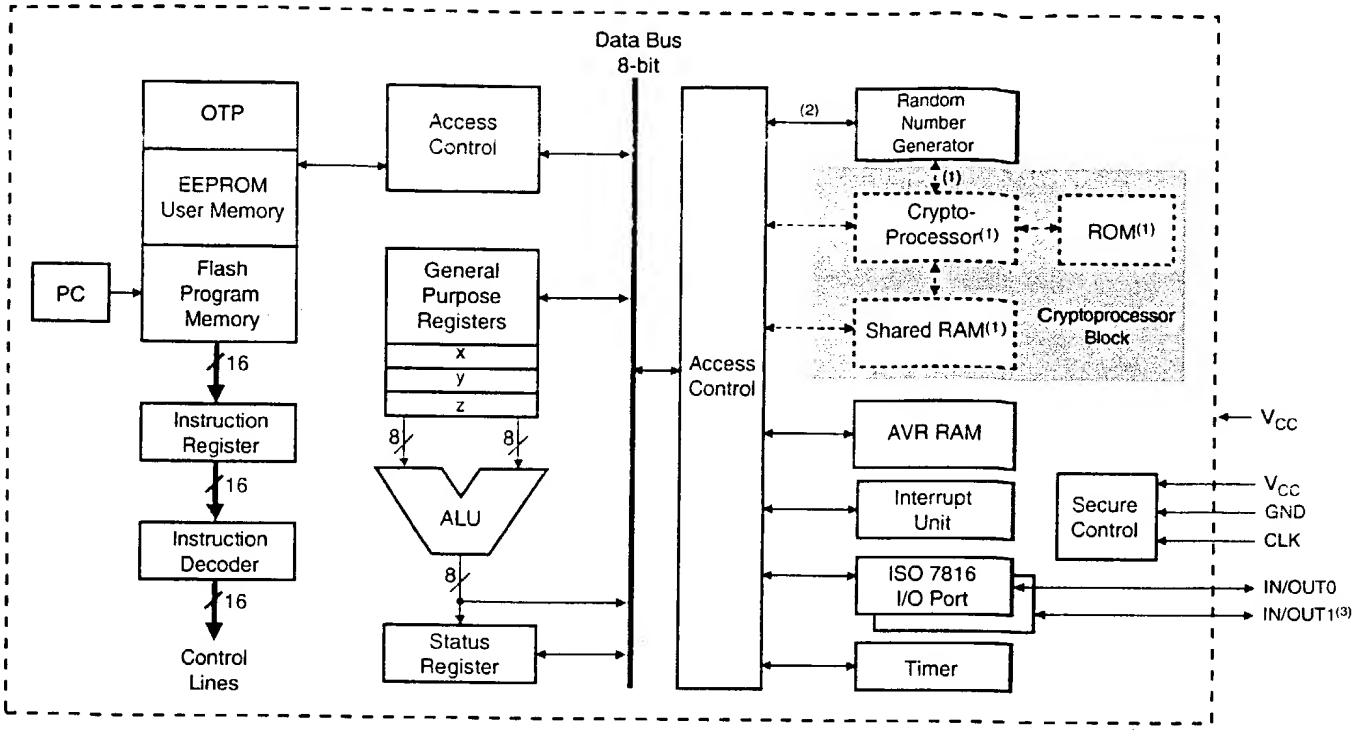
Secure Microcontrollers for Smart Cards

AT90SC Summary

Complete datasheet available under NDA

Rev. 1065CS–10/99

Block Diagram



Note:
1. Only available on products featuring a cryptoprocessor.
2. Only available on products not featuring a cryptoprocessor.
3. Currently available only on AT90SC1616C and AT90SC6464C.

Pin Description

VCC

Supply voltage.

GND

Ground.

RST

Reset input. A low level on this pin for two clock cycles while the AT90SC is running resets the device.
This pin includes an internal pull-up resistor.

CLK

Clock input to internal clock operating circuit.
This pin includes an internal pull-up resistor.

IN/OUT

On products with a single IN/OUT pin, IN/OUT is a single bit open drain bi-directional I/O port. This bi-directional pin includes a pull-up resistor.

Products with a second I/O port can be configured as open drain with pull-up or as a true CMOS I/O port.

8-bit AVR RISC Microcontroller CPU

The AVR uses a Harvard architecture concept with separate memories and buses for program and data. The program memory is accessed with a two stage pipeline. While one instruction is being executed, the next instruction is prefetched from the program memory. This concept enables instructions to be executed in every clock cycle.

The fast-access register file concept contains 32 x 8 general purpose working registers with a single clock cycle access time. This means that during one single clock cycle, one ALU operation is executed. Two operands are output from the register file, the operation is executed, and the result is stored back in the register file in one clock cycle.

The timer and other I/O functions are located in the I/O memory space. The 64 addresses of the I/O memory space can be accessed directly as I/O registers or as memory space.

Memory Organization

The AT90SC microcontrollers have the following memory organization as shown in Figures 1 and 2.

Program memory:

- 16-bit addressable EEPROM user memory
- 16-bit addressable Flash program memory

Data memory:

- 8-bit addressable EEPROM user memory
- 8-bit addressable SRAM shared between AVR and crypto engine
- 8-bit registers addressable as data memory

The EEPROM is shared between program memory and data memory depending on the mode. The portion of EEPROM dedicated to each function is flexible and varies according to the application.

Program memory is read-only in normal operation mode. Both Flash and EEPROM memory locations are directly addressable. The EEPROM memory locations follow the Flash memory in the program address space.

Program Memory

The AT90SC microcontroller has separate address spaces for program memory and data memory. Up to 64K bytes of Flash program memory are available. Figure 1 shows the program memory.

Data Memory

The AT90SC can directly address up to 64K bytes of data memory. The LOAD and STORE instructions access the whole data memory.

The AT90SC family also features 96 bytes of register and I/O space and up to 2.5K bytes of SRAM.

The I/O space of the RAM can be accessed by direct addressing.

The 128-byte last page of the EEPROM user memory is an OTP memory (64 bytes) and bit addressable memory (64 bytes).

Figure 1. The AT90SC Program Memory

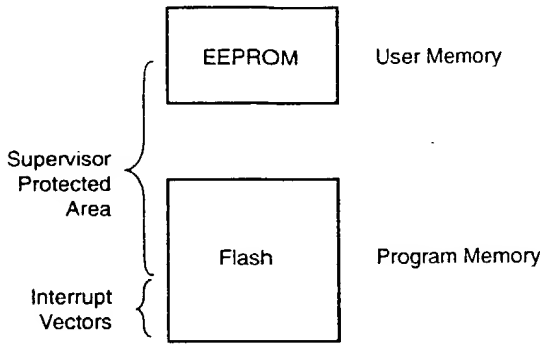
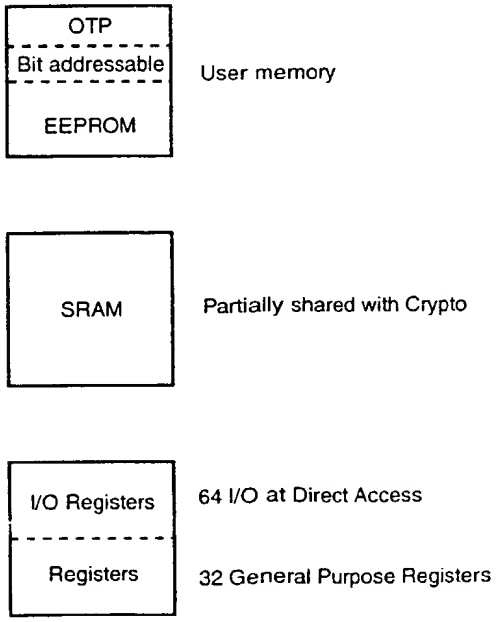


Figure 2. The AT90SC Data Memory



Flash Program Memory

- Page size of 128 bytes
- Minimum endurance of 10K write/erase cycles
- Data retention for a minimum of 40 years

The AT90SC contains up to 64K bytes of downloadable Flash memory for program storage. Since all instructions are 16-bit words, the Flash is organized as 32K x 16. The Flash memory is read-only except during the program download mode. This mode is selected by setting a bit in the memory control I/O register.

Once the Flash memory is loaded, a security feature disables the download function, making the writing of the Flash impossible.

EEPROM User Memory

- Erasure and Writing:
  - Byte-by-byte
  - Bit mode
  - Page mode (128 bytes per page)
- Minimum endurance of 250K write/erase cycles
- Data retention for a minimum of 40 years

The user memory is organized as up to 32K x 16. A write mode bit in the memory control register selects byte by byte or page mode. During the write cycle, a bit is set in the memory control register, disabling pending write operations. When the write cycle is finished, this bit is cleared and an interrupt request is generated.

In addition, the AT90SC features a pseudo bit mode which allows individual bits to be overwritten (one to zero).

Bit Addressable Memory

The 64 bytes of bit addressable memory are found in the last 128-byte page of the EEPROM address space and represent the first 64 bytes of this page.

OTP Memory

The 64 bytes of OTP (One-Time Programmable) Memory are found in the last 128-byte page of the EEPROM address space and represent the last 64 bytes of this page.

Cryptoprocessor

The cryptoprocessor is a 16-bit crypto engine dedicated to performing fast encryption or authentication functions. It is based on a parallel RISC architecture allowing most instructions to be performed in a single clock cycle. The crypto engine can run in parallel with the microcontroller. An internal 16 x 16 multiplier provides 32-bit results within one cycle.

The cryptoprocessor runs on its own internal clock.

The cryptoprocessor ROM stores the program code which contains the following catalog of functions:

- Reset and self test
- Random Number Generation
- Exponentiation with CRT (241 to 1024)
- Exponentiation without CRT (241 to 1024)
- DSA

RAM Memory Sharing

The cryptoprocessor and the AVR share the RAM memory as follows: when the cryptoprocessor is inactive, the entire RAM can be accessed by the CPU. When the cryptoprocessor is active, the shared RAM is not accessible by the CPU.

Operational Modes

The AT90SC features two operational modes:

- A **supervisor mode** with a privileged access to data, active when code is executed from the supervisor memory
- A **user mode** with data access restrictions, active when code is executed from EEPROM user memory

The supervisor and user locations are programmed in I/O registers.

In user mode, direct read and write access to I/O registers and EEPROM is not allowed. Furthermore, a programmable zone in the RAM can be reserved for supervisor mode. Any attempt to access the I/O, EEPROM or reserved RAM area generates a maskable interrupt.

Also, any jump to the supervisor zone in user mode generates a non-maskable security interrupt. The AT90SC provides a supervisor call instruction to branch at a defined vector address of the supervisor zone.

This powerful hardware solution is specially designed to ensure full separation between applications. It provides secure protection against program dumping and secure data access control.

Security Features

For security reasons the following list is not exhaustive.

- Shipping and Initialization are protected by a Transport Code
- Power-down/up protection
- Low-frequency protection against static analysis
- High-frequency protection against intrusion
- Unique serial number
- Supervisor mode
- Secured test structure
- Logical scrambling
- Secure layout

ISO 7816 I/O Ports

The ISO 7816 I/O pins are controlled by the CPU. They can be configured to generate an interrupt on:

- Low level
- Positive edge
- Negative edge
- Positive or negative edge

Interrupt Controller

The AT90SC has a total of six interrupt vectors: security, I/O pins 0 and 1, timer, EEPROM end of write cycle and a cryptoprocessor interrupt.

Each of these interrupt sources can be individually enabled or disabled by setting or clearing a bit in the Interrupt Mask Register located in the I/O memory space. This register also contains a global disable bit which disables all interrupts at once.

One priority level can be programmed in the Interrupt Priority register. A second priority level is given by the vector number.

The interrupt controller is able to memorize interrupts. It sends them to the microcontroller in the correct order according to their priority level.

Reduced Power Mode

To exploit the power savings for smart cards available in CMOS circuitry, Atmel's microcontrollers have two software-invoked reduced power modes.

Idle Mode

During Idle Mode, the CPU is disabled while all on-chip peripherals (RAM, I/O registers, timer and serial port) remain active. This mode is invoked by a SLEEP instruction and by an enabled bit in an I/O register. Idle Mode can be terminated by any enabled interrupt or by a hardware reset.

If a reset occurs during sleep mode, the CPU awakes and executes from the reset vector.

If an interrupt occurs, the CPU awakes and executes the interrupt routine, and resumes execution from the instruction following SLEEP.

Power-down Mode

During Power-down Mode, the clock is frozen. The on-chip RAM and I/O registers retain their values during Power-down Mode. The SLEEP instruction forces this mode. Exit from Power-down can be initiated either by a hardware reset or by the enabled external interrupt. Reset redefines the I/O registers but does not change the on-chip RAM. The I/O registers keep their value if the exit from Power-down is generated by an external interrupt.

Download Mode

The AT90SC microcontroller has a special mode which allows the Flash to be written for new software download. The new software is loaded through the ISO port and written into the Flash memory. This download mode is software controlled, so if the software in use does not contain the download facility, no new program can be loaded. If the product contains only Flash for the code, during program download (OS or application) the code is fetched from the EEPROM.

Timers

The AT90SC provides one or two 16-bit general timers with prescalers. The timers can run on a 16-bit counter or on an 8-bit counter with auto-reload mode.

The Instruction Set

All members of the AT90SC series execute the same instruction set. The 16-bit instruction set provides a variety of fast addressing modes to facilitate byte and word operations on small data structures. The instruction set supports 32 general-purpose registers for efficient implementation of software.

Addressing Mode

The AT90SC AVR RISC microcontroller supports powerful and efficient addressing modes for access to program and data memory:

- Direct I/O addressing
- Direct Register addressing with one or two registers
- Data direct: Operand address is specified by a 16-bit code
- Indirect address data: Operand address is a 16-bit register
- Indirect data with displacement: Operand address is a 16-bit register with a 6-bit offset
- Indirect data with pre-decrement and post-increment: Operand address is a 16-bit register
- Access to program memory: Operand address is a 16-bit register for access in byte LPM instruction
- Indirect program addressing: Operand address is a 16-bit register for IJMP and ICALL
- Relative program addressing: Operand address is a 16-bit PC with an offset of -2048 to +2047
- Direct program addressing

Instruction type

- Data Transfers
  - From/to internal I/O, RAM, Registers
  - From/to internal EEPROM
  - From Flash
- Arithmetic and logical Instruction
  - Manipulation, one or two registers
  - Manipulation, constant and register
- Boolean Instruction
  - Manipulation and test on bit
- Branch instruction
  - Relative branch
  - Indirect branch
  - Conditional skip
  - Unconditional branch
  - Conditional branch
  - Subroutine call and return
  - Interrupt return

Master Clock Generation

The master clock of the CPU is generated by the external ISO 7816 clock.

Development Tools

A complete set of AT90SC development tools and a hardware emulator are available.

Atmel Headquarters

Corporate Headquarters
2325 Orchard Parkway
San Jose, CA 95131
TEL (408) 441-0311
FAX (408) 487-2600

Europe
Atmel U.K., Ltd.
Coliseum Business Centre
Riverside Way
Camberley, Surrey GU15 3YL
England
TEL (44) 1276-686677
FAX (44) 1276-686697

Asia
Atmel Asia, Ltd.
Room 1219
Chinachem Golden Plaza
77 Mody Road
Tsimshatsui East
Kowloon, Hong Kong
TEL (852) 27219778
FAX (852) 27221369

Japan
Atmel Japan K.K.
Tonetsu Shinkawa Bldg., 9F
1-24-8 Shinkawa
Chuo-ku, Tokyo 104-0033
Japan
TEL (81) 3-3523-3551
FAX (81) 3-3523-7581

Atmel Operations

Atmel Colorado Springs
1150 E. Cheyenne Mtn. Blvd.
Colorado Springs, CO 80906
TEL (719) 576-3300
FAX (719) 540-1759

Atmel Rousset
Zone Industrielle
13106 Rousset Cedex, France
TEL (33) 4 42 53 60 00
FAX (33) 4 42 53 60 01

Fax-on-Demand
North America:
1-(800) 292-8635

International:
1-(408) 441-0732

e-mail
literature@atmel.com

Web Site
http://www.atmel.com

BBS
1-(408) 436-4309

1065CS–10/99/5M